CLAIMS

What is claimed is:

1. A method of transmitting same data to a plurality of destinations by email, comprising the steps of:

(a) encrypting data by utilizing a session key;

(b) encrypting the session key by utilizing each of common keys which have been determined to the respective destinations; and

(c) transmitting email including the encrypted data and the encrypted session key.

2. The method according to claim 1,

wherein in the step (c), the email including header information showing the plurality of the destinations as well as the encrypted data and the encrypted session key is transmitted.

3. The method according to claim 1,

wherein in the step (c), the email including the encrypted data and the one encrypted session key is transmitted to a destination related to the common key which has been utilized to encrypt the one session key.

4. The method according to claim 1,

wherein in the step (b), before transmitting the email, the session key is repeatedly encrypted until all of the common keys which have been determined to the respective destinations are utilized to encrypt the session key, and

wherein in the step (c), the email including the encrypted data and all of the encrypted session keys is transmitted to all of the destinations by one transmission process.

5. The method according to claim 1,

wherein until all of the common keys which have been determined to the respective destinations are utilized to encrypt the session key, steps (b) and (c) are repeated such that after transmitting the email, the session key is encrypted by another common key, and then another email including the encrypted data and the session key encrypted by the another common key is transmitted.

6. The method according to claim 1, further including the step of generating each of the common keys by utilizing each public key generated based on information of each of the plurality of the destinations and utilizing a secret key.

7. The method according to claim 6, wherein the common key is generated by ID-based Non-Interactive Key Sharing Scheme.

8. The method according to claim 1,

wherein the data and the session key are encrypted by Data Encryption Standard.

9. A device for transmitting email comprising:

first means for encrypting data by utilizing a session key;

second means for encrypting the session key by utilizing each of common keys which have been determined to the respective destinations; and

third means for transmitting email including the encrypted data and the encrypted session key.

10. The device for transmitting email according to claim 9,

wherein third means transmits the email including header information showing the plurality of the destinations as well as the encrypted data and the encrypted session key.

11. The device for transmitting email according to claim 9,

wherein the third means transmits the email including the encrypted data and the one encrypted session key to a destination related to the common key which has been utilized to encrypt the one session key.

12. The device for transmitting email according to claim 9,

wherein before the third means transmits the email, the second means encrypts the session key repeatedly until all of the common keys which have been determined to the respective destinations are utilized to encrypt the session key, and

wherein the third means transmits the email including the encrypted data and all of the encrypted session keys to all of the destinations by one transmission process.

13. The device for transmitting email according to claim 9,

wherein until all of the common keys which have been determined to the respective destinations are utilized to encrypt the session key, the second means and the third means repeat encryption of the session key and transmission of the email respectively such that after transmitting the email, the session key is encrypted by another common key, and then another email including the encrypted data and the session key encrypted by the another common key is transmitted.

14. The device for transmitting email according to claim 9, further including means for generating each of the common keys by utilizing each public key generated based on information of each of the plurality of the destinations and utilizing a secret key.

15. A storing medium storing a program for causing a computer to transmit same data to a plurality of destinations, wherein the program includes:

first program code means for causing a computer to encrypt data by utilizing a session key;

second program code means for causing the computer to encrypt the session key by utilizing each of common keys which have been determined to the respective destinations; and

third program code means for causing the computer to transmit email including the encrypted data and the encrypted session key.

16. The storing medium according to claim 15,

wherein third program code means causes the computer to transmit the email including header information showing the plurality of the destinations as well as the encrypted data and the encrypted session key.

17. The storing medium according to claim 15,

wherein the third program code means causes the computer to transmit the email including the encrypted data and the one encrypted session key to a destination related to the common key which has been utilized to encrypt the one session key.

18. The storing medium according to claim 15,

wherein before the third program code means causes the computer to transmit the email, the second program code means causes the computer to encrypt the session key repeatedly until all of the common keys which have been determined to the respective destinations are utilized to encrypt the session key, and

wherein the third program code means causes the computer to transmit the email including the encrypted data and all of the encrypted session keys to all of the destinations by one transmission process.

19. The storing medium according to claim 15,

wherein until all of the common keys are utilized to encrypt the session key, the second program code means and the third program code means causes the computer to repeat encryption of the session key and transmission of the email respectively such that after transmission of the email, the session key is encrypted by another common key, and then another email including the encrypted data and the session key encrypted by the another common key is transmitted.

20. The storing medium according to claim 15, further including fourth program code means for causing the computer to generate each of the common keys by utilizing each public key generated based on information of each of the plurality of the destination and utilizing a secret key.